CHAPTER 1

SYSTEMS OF RECORDS

A. GENERAL

1. System of records. To be subject to the provisions of this Regulation a "system of records" must

a. Consist of "records" (as defined in paragraph 13, page xii) that are retrieved by the name of an individual ***or*** some other personal identifier, and

b. Be under the control of a DoD Component.

2. Retrieval practices

a. Records in a group of records that may be retrieved by a name or personal identifier are not covered by this Regulation even if the records contain personal data and are under control of a DoD Component. The records must be, in fact, retrieved by name or other personal identifier to become a system of records for the purpose of this Regulation.

b. If files that are not retrieved by name or personal identifier are rearranged in such manner that they are retrieved by name or personal identifier, a new systems notice must be submitted in accordance with subsection D.3. of Chapter 6.

c. If records in a system of records are rearranged so that retrieval is no longer by name or other personal identifier, the records are no longer subject to this Regulation and the system notice for the records shall be deleted in accordance with subsection E.3. of Chapter 6.

3. Relevance and necessity. Retain in a system of records only that personal information which is relevant and necessary to accomplish a purpose required by a federal statute or an Executive Order.

4. Authority to establish systems of records. Identify the specific statute or the Executive Order that authorizes maintaining personal information in each system of records. The existance of a statute or Executive order mandating the maintenance of a system of records does not abrogate the responsibility to ensure that the information in the system of records is relevant and necessary.

5. Exercise of First Amendment rights

a. Do not maintain any records describing how an individual exercises his or her rights guaranteed by the First Amendment of the U.S. Constitution except when:

(1) Expressly authorized by federal statute;

(2) Expressly authorized by the individual; or

(3) Maintenance of the information is pertinent to and within the scope of an authorized law enforcement activity.

b. First Amendment rights include, but are not limited to, freedom of religion, freedom of political beliefs, freedom of speech, freedom of the press, the right to assemble, and the right to petition.

6. System manager's evaluation

a. Evaluate the information to be included in each new system before establishing the system and evaluate periodically the information contained in each existing system of records for relevancy and necessity. Such a review shall also occur when a system notice amendment or alteration is prepared (see sections D. and E. of Chapter 6).

b. Consider the following:

(1) The relationship of each item of information retained and collected to the purpose for which the system is maintained;

(2) The specific impact on the purpose or mission of not collecting each category of information contained in the system;

(3) The possibility of meeting the informational requirements through use of information not individually identifiable or through other techniques, such as sampling;

(4) The length of time each item of personal information must be retained;

(5) The cost of maintaining the information; and

(6) The necessity and relevancy of the information to the purpose for which it was collected.

i'. Discontinued information requirements

a. Stop collecting immediately any category or item of personal information for which retention is no longer justified. Also excise this information from existing records, when feasible.

b. Do not destroy any records that ❑ust be retained in accordance with disposal authorizations established under 44 U.S.C., Section 303a (reference (c)).

B . STANDARDS OF ACCURACY

1. Accuracy of information maintained. Maintain all personal information that is used or may be used to make any determination about an individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual in making any such determination.

2. Accuracy determinations before dissemination. Before disseminating any personal information from a system of records to any person outside the Depart-

ment of Defense, other than a federal agency, make reasonable efforts to ensure that the information to be disclosed is accurate, relevant, timely, and complete for the purpose it is being maintained (see also subsection A.4. of Chapter 3 and subsection A.4. of Chapter 4).

C. GOVERNMENT CONTRACTORS

1. Applicability to government contractors

a. When a DoD Component contracts for the operation or maintenance of a system of records or a portion of a system of records by a contractor, the record system or the portion of the record system affected are considered to be maintained by the DoD Component and are subject to this Regulation. The Component is responsible for applying the requirements of this Regulation to the contractor. The contractor and its employees are to be considered employees of the DoD Component for purposes of the sanction provisions of the Privacy Act during the performance of the contract. Consistent with the Defense Acquisition Regulation (DAR), ***section*** 1.327 (reference (d)), contracts requiring the maintenance of a system of records or the portion of a system of records shall identify specifically the record system and the work to be performed and shall include in the solicitation and resulting contract such terms as are prescribed by reference (d).

b. If the contractor must use or have access to individually identifiable information subject to this Regulation to perform any part of a contract, and the information would have been collected and maintained by the DoD Component but for the award of the contract, these contractor activities are subject to this Regulation.

c. The restriction in paragraphs C.1.a. and b. of this Chapter do not apply to records:

(1) Established and maintained to assist in making internal contractor management decisions, such as records maintained by the contractor for use in managing the contract;

(2) Maintained as internal contractor employee records even when used in conjunction with providing goods and services to the Department of Defense; or

(3) Maintained as training records by an educational organization contracted by a DoD Component to provide training when the records of the contract students are similar to and comingled with training records of other students (for example, admission forms, transcripts, academic counseling and similar records).

(4) Maintained by a consumer reporting agency to which records have been disclosed under contract in accordance with the Federal Claims Collection Act of 1966 (reference (e)).

d. DoD Components must publish instructions that:

(1) Furnish DoD Privacy Program guidance to their persomel who solicit, award, or administer government contracts;

(2) Inform prospective contractors of their responsibilities regarding the DoD Privacy Program; and

(3) 'Establish an internal system of contractor performance review to ensure compliance with the DoD Privacy Program. "

2. Contracting procedures. The Defense Systems Acquisition Regulatory Council (DSARC) is responsible for developing the specific policies and procedures to be followed when soliciting bids, awarding contracts or administering contracts that are subject to this Regulation.

3. Contractor compliance. Through the various contract surveillance programs, ensure contractors comply with the procedures. established in accordance with subsection C.2. of this Chapter.

4. Disclosure of records to contractors. Disclosure of personal records to a contractor for the use in the performance of any DoD contract by a DoD Component is considered a disclosure within the Department of Defense (see subsection A.2. of Chapter 4). The contractor is considered the agent of the contracting DoD Component and to be maintaining and receiving the records for that Component.

D. SAFEGUARDING PERSONAL INFORMATION

1. General responsibilities. Establish appropriate administrative, technical and physical safeguards to ensure that the records in every system of records are protected from unauthorized alteration or disclosure and that their confidentiality is protected. Protect the records against reasonably anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom information is kept.

2. Minimum standards

a. Tailor system safeguards to conform to the type of records in the system, the sensitivity of the personal information stored, the storage medium used and, to a degree, the number of records maintained.

b. Treat all unclassified records that contain personal information that normally would be withheld from the public under Exemption Numbers 6 and 7, section 3-200, DoD 5400.7-R (reference (f)) as if they were designated "For Official Use Only" and safeguard them in accordance with the standards established by reference (f) even if they are not actually marked "For Official Use Only."

c. Afford personal information that does not meet the criteria discussed in paragraph D.3.b. of this Chapter that degree of security which provides protection commensurate with the nature and type of information involved.

d. Special administrative, physical, and technical procedures are required to protect **data** that is stored or being processed temporarily in an

automated data processing (ADP) system or in a word processing activity to protect it against threats unique to those environments (see Appendices A and B).

e. Tailor safeguards specifically to the vulnerabilities of the system.

3. Records disposal

a. Dispose of records containing personal data so as to prevent inadvertent compromise. Disposal methods such as tearing, burning, melting, chemical decomposition, pulping, pulverizing, shredding, ***or*** mutilation are considered adequate if the personal data is rendered unrecognizable or beyond reconstruction.

b. The transfer of large quantities of records containing personal data (for example, computer cards and printouts) in bulk to a disposal activity, such as the Defense Property Disposal Office, is not a release of personal information under this Regulation. The sheer volume of such transfers make it difficult or impossible to identify readily specific individual records (see paragraph D.3.c. of this Chapter).

c. When disposing of or destroying large quantities of records containing personal information, care must be exercised to ensure that the bulk of the records is maintained so as to prevent specific records from being readily identified. If bulk is maintained, no special procedures are required. If bulk cannot be maintained or if the form of the records make individually identifiable information easily available, dispose of the record in accordance with paragraph D.3.a. of this Chapter.